[0005]

[PROBLEM TO BE SOLVED BY THE INVENTION]

The conventional technique has disadvantages. Assuming that private communication have already been performed between terminals, if a new logic path is generated to perform private communication, it is necessary to perform authentication between the terminals again, and the overhead is large. Further, assuming that a certificate is used for authentication between the terminals, when private communication is performed after finishing authentication between the terminals and sharing of a secret key, and establishing a communication path, if an additional communication path is newly established for performing private communication, the following problem occurs.

Specifically, it happens that when the certificates were exchanged between the terminals for establishing the communication path for the previous private communication, the opponent's certificate was valid, but when authentication between the terminals is performed for the communication path to establish the new private communication, the opponent's certificate has expired. Therefore, even if the terminals performing the private communication are not changed, a status discrepancy problem occurs, i.e., the communication path for the previous communication is valid, and the communication path for the new communication has expired.

[0006]

The present invention has been made to solve the problem, and an object of the present invention is to provide a method of authentication and key sharing for suitable private communication when a digital transmission path is used, and data information is transmitted.

[0007]

[MEANS FOR SOLVING THE PROBLEM]

In the present invention, each of terminal devices stores a certificate as information for certifying that the terminal device itself is a legitimate device. The certificate comprises digital information including an identification name of the terminal and a public key in a public key cryptosystem of the terminal, and the digital information has been digitally signed using a private key in a public key cryptosystem of a certification organization. When private communication is performed between terminal devices each storing the certificate, the terminal devices perform the following process. Firstly, the certificates of the terminal devices are exchanged for authenticating that the opponent terminal is a legitimate device. Then, a secret key in a secret key cryptosystem used for encryption/decryption of the content of communication data is shared using the public key cryptosystem. The shared secret key for communication is used to perform private communication.

[0008]

It is assumed that a terminal device Ti and a terminal device Tj perform private communication. Firstly, the terminal devices Ti, Tj establish a communication path for authenticating each other, and exchange certificates Ci, Cj certifying the terminal devices Ti, Tj, and verify the exchanged certificates Ci, Cj. Thus, each of the terminal devices Ti, Tj confirms that the opponent is legitimate, and the communication path established for authentication is legitimate.

[0009]

Next, a communication path for encryption/decryption of the content of communication data is established at a level above the communication path established for authentication. In order to share the secret key for encryption/decryption of the content of communication data, the terminal device Ti generates a random number Rkvi, and encrypts the random number Rkvi using a public key of the terminal device Tj extracted from the certificate Cj obtained at the time of authenticating the terminal device Tj. The terminal device Ti further encrypts the encrypted data or the data obtained by hashing the encrypted data using the private key of the terminal device Ti for adding the digital signature data. The digital information containing the encrypted data and the digital signature data is transmitted to the terminal device Tj.

[0010]

When the terminal device Tj receives the digital information, the terminal device Ti decrypts the digital data of the random number Rkvi encrypted using the public key of the terminal device Tj in the received digital information, using the private key of the terminal device Tj to obtain a value of the random number Rkvi. Further, the terminal device Tj decrypts the digital signature data using the public key of the terminal device Ti extracted from the certificate Ci obtained at the time of authenticating the terminal device Ti, and compares the decrypted digital data with the digital data of the random number Rkvi encrypted using the public key of the terminal device Tj. If these digital data are the same, the terminal device Tj determines that the received digital information is legitimate, and the terminal device Tj confirms that the digital information is the secret key information sent from the terminal device Ti. Then, the terminal device Tj generates the random number Rkvi and performs an XOR operation using the random number Rkvj and the decrypted random number Rkvi, and determines the result of the operation as a secret key for communication in the secret key cryptosystem and the other necessary data (initial value). Further, the terminal device Tj encrypts the random number Rkvj using the public key of the terminal Ti extracted from the certificate obtained at the time of authenticating the terminal Ti, and encrypts the encrypted data or the data obtained by hashing the

encrypted data using the private key of the terminal device Tj for adding the digital signature data. The digital information containing the encrypted data and the digital signature data is transmitted to the terminal device Ti.

[0011]

When the terminal device Ti receives the digital information, the terminal device Ti decrypts the digital data of the random number Rkvj encrypted using the public key of the terminal device Ti in the received digital information, using the private key of the terminal device Ti to obtain a value of the random number Rkvj. Further, the terminal device Tj decrypts the digital signature data using the public key of the terminal device Tj extracted from the certificate Cj obtained at the time of authenticating the terminal device Tj, and compares the decrypted digital data with the digital data of the random number Rkvj encrypted using the public key of the terminal device Tj. If these digital data are the same, the terminal device Tj determines that the received digital information is legitimate, and the terminal device Tj confirms that the digital information is the secret key information sent from the terminal device Tj. Then, the terminal device Ti generates the random number Rkvi and performs an XOR operation using the previously generated random number Rkvi and the random number Rkvj, and determines the result of the operation as a secret key for

communication in the secret key cryptosystem and the other necessary data (initial value).

[0012]

Thus, the terminal device Ti and the terminal device Tj share the secret key and other data (initial value) used for encryption of the same communication data content, and use the shared key and other data for encryption and decryption of the content of communication data in the secret key cryptosystem.

[0013]

Further, in the present invention, a plurality of communication paths for encryption/decryption of the content of communication data are established at the level above the communication path established for authentication. When private communication is performed using the communication paths for encryption/decryption of the content of the respective items of communication data, the secret key is shared in each of the communication paths for encryption/decryption of the content of communication data. Thus, it is possible to perform private communication through a plurality of communication paths using various secret keys, which are established on one communication path for authentication.

[0014]

Further, in the present invention, if at least one communication path for encryption/decryption of the content of communication data is established at the level

above the communication path for authentication, when a communication path for encryption/decryption of the content of new communication data is established on the communication path for authentication, information of the certificate of the previously established authentication path is used as information of the certificate for sharing a new secret key and the other data which are newly required for private communication.

[0015]

Further, in the present invention, at the time of finishing private communication, when all the communication paths for encryption/decryption of the content of communication data established on the communication path for authentication are closed, the information on the communication path for authentication is closed.

[0016]

[EMBODIMENET]

Hereinafter, an embodiment of the present invention will be described with reference to the drawings. In the description of the embodiment, ISDN is used as a digital transmission path. Alternatively, it is a matter of course that the present invention is applicable to digital transmission paths other than ISDN.

[0017]

FIG. 1 is a block diagram showing an embodiment of a communication system to which a private communication

method according to the present invention is applied. In FIG. 1, a switching device 10 accommodates a plurality of ISDN basic interface subscriber lines. The terminal devices 20, 30 are connected to the ISDN basic interface subscriber lines. Each of the terminal devices includes a terminal control unit 110, an encryption processing unit 120, and a communication data processing unit 130. The terminal control unit 110 performs network control of layers 1 to 3 for the ISDN subscriber lines and upper layers, i.e., a layer 4 and higher. The encryption processing unit 120 performs the authentication process and the key sharing process between the terminals. The communication data processing unit 130 performs private communication using the shared secret key. Further, the terminal devices 20, 30 are connected to a certification organization 40. Each of the terminal devices 20, 30 receives a digitally signed certificate issued by the certification organization 40 for the digital information comprising the identification name of the terminal device and the public key of the terminal device. If the users directly go to the certification organization 40 to receive the certificate, connections between the terminal devices 20, 30 and the certification organization 40 may be omitted. In the following description, the terminal device 20 is denoted by Ti, and the terminal device 30 is denoted by Tj.

[0018]

FIG. 2 is an example of signs used in the embodiment of the present invention. As for the signs for the terminal Tj, the alphabet "i" in FIG. 2 can be substituted with the alphabet "j".

[0019]

FIG. 3 is an example of a certificate generated by the certification organization 40. For example, the certificate Ci of the terminal Ti includes the length CDL of the certificate, an identification name Ti of the terminal device, a public key Pki in the public key cryptosystem of the terminal Ti, and a code E[Sca] (H(Ti||Pki)). The information obtained by combining the identification name Ti and the public key Pki is hashed using one way data compression function H, and the value is encrypted using a private key Sca in the public key cryptosystem of the certification organization 40 to produce the code E[Sca] (H(Ti||Pki)). That is, the certificate Ci is the digitally signed data. Typically, the RSA cryptosystem (see document [6]: "PKCS#1 RSA Encryption Standard, Version 1.5, RSA data security Inc. 1993", for details) is an example of the public key cryptosystem, and the DES cryptosystem (see document [7]: "FIPS Publication 46-1: Data Encryption Standard, National Bureau of Standards, 1988" for details) is an example of the secret key cryptosystem. Further, MD2 (document [8]: "RCF1319: The MD2 Message-Digest Algorithm., B. Kaliski., 1992", for details) and MDS5 (document [9]: "RFC1321 The

MD5 Message Digest Algorithm., B. Kaliski., 1992", for details) are examples of the hash function. It is a matter course that the present invention is applicable to other public key cryptosystems, secret key cryptosystems, and hush functions.

[0020]

At the time of terminal installation, the terminal 20 (terminal Ti) generates the public key Pki and the private key Ski of the terminal, and sends the identification name Ti of the terminal and the public key Pki to the certification organization 40 for receiving the certificate Ci issued by the certification organization 40. The terminal 20 (terminal Ti) sets the private key Ski of the terminal, the certificate Ci shown in FIG. 2, and the public key Pca of the certification organization 40 in the encryption processing unit 120. Likewise, the terminal 30 (terminal Tj) sets the private key Skj of the terminal, the certificate Cj, and the public key Pca of the certification organization 40 in the encryption processing unit 120.

[0021]

When the terminal 20 (Ti) and the terminal 30 (Tj) perform private communication, firstly, the certificates Ci, Cj of these terminals are exchanged to determine that the opponent is legitimate. Then, the secret key in the private key cryptosystem used for encryption/decryption of the content of communication data is shared using the

public key cryptosystem, and the shared private key is used to perform private communication.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-074408
(43)Date of publication of application : 18.03.1997

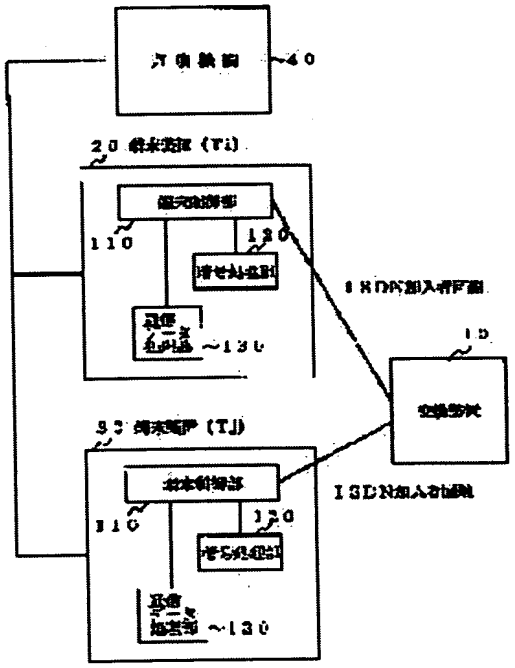
(51)Int.CI. H04L 9/08
G09C 1/00
G09C 1/00
H04L 9/32

(21)Application number : 07-226267
(22)Date of filing : 04.09.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
N T T ELECTRON TECHNOL KK
(72)Inventor : TANAKA KIYOTO
AOKI KATSUHIKO

(54) SECURITY COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate an overhead for a verification procedure between terminal equipments and to prevent contradiction from being incurred between communication channels for ciphering/decoding communication data.
SOLUTION: Terminal equipments 20, 30 hold a certificate signed digitally by a private key of a verification agency 40 with respect to an identification name of the terminal equipments and digital information of a public key as information to verify it that the terminal equipments are correct. In the case of security communication by the terminal equipments 20, 30, at first a channel to verify the terminal equipments with each other is open and each certificate is exchanged mutually to confirm the correctness of the opposite party. Then a communication channel for ciphering/decoding of the communication data is open for a higher layer of the communication channel opened for verification and a secret key of the correct key ciphering system is used in common by using the open public key ciphering system.



LEGAL STATUS

[Date of request for examination] 11.04.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3453944

[Date of registration] 25.07.2003
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－74408

(43)公開日　平成９年(1997)３月18日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｃ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｃ
			7259－5Ｊ			６３０Ｅ
		６４０	7259－5Ｊ			６４０Ａ
			7259－5Ｊ			６４０Ｅ

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願平7－226267

(22)出願日　平成７年(1995)９月４日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(71)出願人　591230295
エヌティティエレクトロニクステクノロジー株式会社
東京都武蔵野市吉祥寺本町１丁目14番５号

(72)発明者　田中　清人
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　鈴木　誠

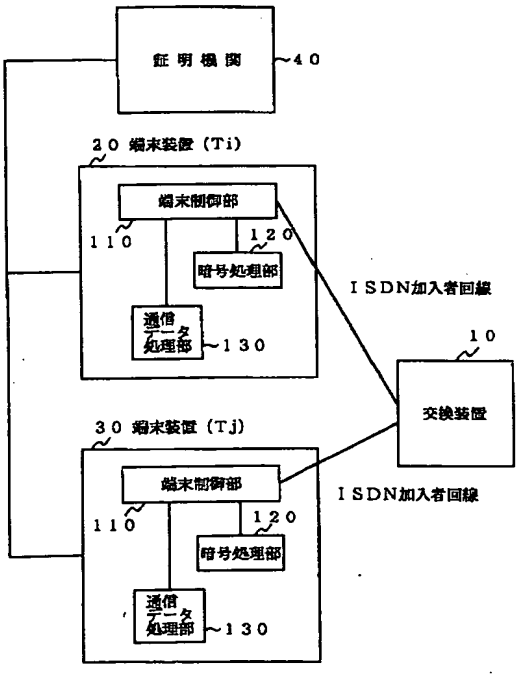
最終頁に続く

(54)【発明の名称】　秘話通信方法

(57)【要約】

【課題】　端末相互の認証手順のオーバヘッドをなくし、また、通信データの暗号化／復号のための通信路相互で矛盾を生じないようにする。

【解決手段】　端末装置２０，３０は、当該端末自身が正しいことを証明するための情報として、端末の識別名と端末のパブリック鍵のディジタル情報に対して証明機関４０のプライベート鍵によりディジタル署名された証明書を保持する。端末装置２０，３０が秘話通信を行う場合、まず、相互に認証を行うための通信路を開設し、証明書を相互に交換して相手が正しいと確認する。次に、上記認証のために開設した通信路の上位に通信データの暗号化／復号を行うための通信路を開設し、秘密鍵暗号方式の秘密鍵を公開鍵暗号方式を使用して共有する。



【特許請求の範囲】
【請求項１】　各端末装置は、端末装置自身が正しいことを証明するための情報として、端末装置の識別名と端末装置の公開鍵暗号方式におけるパブリック鍵とで構成されたディジタル情報に対して証明機関の公開鍵暗号方式のプライベート鍵によりディジタル署名された証明書を保持し、端末装置相互が秘話通信を行うとき、まず端末装置が保持する前記証明書を相互に交換して相手が正しいと認証し、次に通信データの内容の暗号化／復号に使用するための秘密鍵暗号方式における秘密鍵を公開鍵暗号方式を使用して共有し、該相互に共有した通信用の秘密鍵を使用して秘話通信を行う方法において、
端末装置Ｔiと端末装置Ｔjが秘話通信を行うとき、まず、端末装置Ｔi，Ｔjは相互に認証を行うための通信路を開設し、自分を証明する証明書Ｃi，Ｃjを互いに交換し検証することで、相手が正しいことを確認するとともに認証のために開設した通信路が正しいことを確認し、
次に、認証のために開設した通信路の上位に通信データの内容の暗号化／復号を行うための通信路を開設し、通信データの内容の暗号化／復号のための秘密鍵を共有するために、端末装置Ｔiは乱数Ｒkviを発生し、該乱数Ｒkviを端末装置Ｔjの認証時に取得した証明書Ｃjから取り出した端末装置Ｔjのパブリック鍵を使用して暗号化するとともに、該暗号化データに対して端末装置Ｔiのプライベート鍵で暗号化することでディジタル署名を行い、これら暗号化データとディジタル署名データのディジタル情報を端末装置Ｔjに送信し、
前記ディジタル情報を受信した端末装置Ｔjは受信したディジタル情報中の端末装置Ｔjのパブリック鍵により暗号化された乱数Ｒkviのディジタルデータを端末装置Ｔjのプライベート鍵により復号することにより乱数Ｒkviの値を得るとともに、ディジタル署名データを端末装置Ｔiの認証時に取得した証明書Ｃiから取り出した端末装置Ｔiのパブリック鍵を使用して復号し、該復号したディジタルデータと前記端末装置Ｔjのパブリック鍵により暗号化された乱数Ｒkviのディジタルデータを比較し、等しければ正しく端末装置Ｔiより送信された秘密鍵情報であると確認し、
次に、端末装置Ｔjは乱数Ｒkvjを生成し、該生成した乱数Ｒkvjと前記復号した乱数Ｒkviとの排他的論和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータとし、さらに前記乱数Ｒkvjを前記端末装置Ｔiの認証時に取得した証明書Ｃiから取り出した端末装置Ｔiのパブリック鍵を使用して暗号化するとともに、該暗号化データに対して端末装置Ｔjのプライベート鍵で暗号化することでディジタル署名を行い、これら暗号化データとディジタル署名データディジタル情報を端末装置Ｔiに送信し、
前記ディジタル情報を受信した端末装置Ｔiは、受信したディジタル情報中の端末装置Ｔiのパブリック鍵により暗号化された乱数Ｒkvjのディジタルデータを端末装置Ｔiのプライベート鍵により復号することにより乱数Ｒkvjの値を得るとともに、ディジタル署名データを端末装置Ｔjの認証時に取得した証明書Ｃjから取り出した端末装置Ｔjのパブリック鍵を使用して復号し、該復号したディジタルデータと前記端末装置Ｔjのパブリック鍵により暗号化された乱数Ｒkvjのディジタルデータを比較し、等しければ正しく端末装置Ｔjより送信された鍵情報であると確認し、
次に、端末装置Ｔiは前記生成した乱数Ｒkviと前記復号した乱数Ｒkvjとの排他的論理和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータとし、
端末装置Ｔiと端末装置Ｔjは、前記共有した秘密鍵と他のデータを使用して秘密鍵暗号方式で通信内容の暗号化ならびに復号を行うことを特徴とする秘話通信方法。
【請求項２】　請求項１記載の秘話通信方法において、通信データの内容の暗号化／復号のための通信路は、認証のために開設した通信路の上位に複数本開設可能し、各通信データの内容の暗号化／復号の通信路で秘話通信を行うときは、各々の通信データの内容の暗号化／復号のための通信路で秘密鍵を共有することで、一つの認証のための通信路上で、各々異なる秘密鍵を使用して複数の通信路で秘話通信を行うことを特徴とする秘話通信方法。
【請求項３】　請求項２記載の秘話通信方法において、通信データの内容の暗号化／復号のための通信路が、認証のための通信路の上位に少なくともひとつ開設してあれば、該認証ための通信路上に新しい通信データの内容の暗号化／復号のための通信路を開設するとき、秘話通信を行うために新たに必要な秘密鍵と他のデータを共有するために使用する証明書の情報は、既に開設している認証のための通信路の証明書の情報を使用することを特徴とする秘話通信方法。
【請求項４】　請求項３記載の秘話通信方法において、秘話通信を終了するとき、認証のための通信路上に開設された全ての通信データの内容の暗号化／復号のための通信路が閉設されたときに、該認証のための通信路上の情報を閉設することを特徴とする秘話通信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタル伝送路を使用して端末装置間で秘話通信を行う方法に関し、特に、ディジタル伝送路を使用して、データ情報を転送する場合にあたって好適な相互の認証方法ならびに通信内容の暗号化／復に使用する鍵ならびにその他の秘密情報を共有する方法に関するものである。
【０００２】
【従来の技術】ディジタル通信のセキュリティ対策として秘話通信がある。秘話通信では、送信者と受信者が互いに相手が正しいと確認した上で秘話通信を行う。

【０００３】秘話通信を行うための暗号方式は、大きく分けて、秘密鍵暗号方式と公開鍵暗号方式の二つがある。公開鍵暗号方式は、暗号化鍵と復号鍵が同じで、この同じ秘密の鍵（以後秘密鍵と呼ぶ）を送信者と受信者が共有して相互に暗号化と復号を行う（詳細は、文献［１］：「現代暗号理論：池野信一、小山謙二著、電子情報通信学会、ＰＰ２４～４０、１９８８」を参照）。一方、公開鍵暗号方式は、暗号化鍵と復号鍵が異なり、復号鍵だけを秘密（以下プライベート鍵と呼ぶ）にするが、暗号化鍵を公開（以下パブリック鍵と呼ぶ）にする方式である（詳細は文献［１］：「現代暗号理論：池野信一、小山謙二著、電子情報通信学会、ＰＰ７７～１０４、１９８８」を参照）。

【０００４】公開鍵暗号方式は、パブリック鍵を知っている誰もが秘話通信の送信者になれる点や、プライベート鍵を知っているただ一人が署名できる点で秘密鍵暗号方式より優れているが、計算量が膨大なため絞号化速度が遅いという欠点がある。このため現状では、送受信者相互の認証と通信データの内容の暗号化／復号の双方に秘密鍵暗号方式を使用するか（例えば、文献［２］：「山口他、ＬＡＮ暗号通信の実装と証価、電子情報通信学会技術研究報告、ＯＳＦ９３－３８，１９９３」を参照）、あるいは送受信者相互の認証には公開鍵暗号方式を使用し、通信データの内容の暗号化／復号には秘密鍵暗号方式を使用する（例えば、文献［３］：「Ｊ．Ｌｉｎ．ＲＦＣ1421：Ｐｒｉｖａｃｙ Ｅｎｈａｎｃｅｍｅｎｔ ｆｏｒ Ｉｎｔｅｒｎｅｔ ＥｌｅｃｔｒｏｎｉｃＭａｉｌ：Ｐａｒｔｌ：Ｍｅｓｓａｇｅ Ｅｎｃｒｙｐｌｉｏｎ ａｎｄ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｃｃｅｄｕｒｅｓ．Ｆｅｂｒｕａｒｙ １９９３．」を参照）方法が使用されている。ここで、秘密鍵暗号方式ならびに公開鍵暗号方式による端末相互の認証方法については、例えば、文献［４］（“Ｉｎｆｏｍａｔｉｏｎ ｔｅｃｈｎｏｌｏｇｙ-Ｓｅｃｕｒｉｔｙ ｔｅｃｈｎｉｑｕｅｓ-Ｅｎｔｉｔｙ ａｕｔｈｅｎｔｉｃａｔｉｏｎ-Ｐａｒｔ ２：Ｍｅｃｈａｎｉｓｍｓ ｕｓｉｎｇ ｓｙｍｅｔｒｉｃ ｅｎｃｉｐｈｅｒｍｅｎｔ ａｌｇｏｒｉｔｈｍｓ”ＩＳＯ／ＩＥＣ ９７９８-２：１９９４）や文献［５］：（“Ｉｎｆｏｍａｔｉｏｎ ｔｅｃｈｎｏｌｏｇｙ-Ｓｅｃｕｒｉｔｙ ｔｅｃｈｎｉｑｕｅｓ-Ｅｎｔｉｔｙ ａｕｔｈｅｎｔｉｃａｔｉｏｎ-Ｐａｒｔ ２：Ｅｎｔｉｔｙ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｕｓｉｎｇ ａ ｐｕｂｌｉｃ ｋｅｙ ａｌｇｏｒｉｔｈｍｓ”ＩＳＯ／ＩＥＣ ９７９８-３：１９９４）に詳述されている。これらの端末相互の認証を使用する従来方法では、認証後に秘話通信を行う場合、認証に使用した通信路そのものを通信データの内容の暗号化／復号に使用する。

【０００５】

【発明が解決しようとする課題】上述の従来技術においては、既に秘話通信を行っている端末相互で、近たな論理パスを生成して秘話通信を行うには再度端末相互の認証を行わなければならず、オーバヘッドが大きいという欠点がある。また、端末相互の認証に証明書を使用する場合、既に端末相互に認証ならびに秘密鍵の共有を終了し通信用のパスを確立して秘話通信を行っている時に、新たにもう一つの通信用のパスを確立して秘話通信を行うには、次のような問題が生じる。すなわち、既設の秘話通信のための通信パスの確立のために互いに証明書の交換を行い認証を行ったときは相手の証明書の期限はまだ切れていなかったが、新たに開設する秘話通信のための通信用のパスのために相互に認証を行った時は、相手の証明書の期限が切れており、同じ端末同士で秘話通信を行うにもかかわらず、既設の通信用のパスは期限内であるが、新たに開設する通信用のパスは期限が切れているという状態不一致の問題が生じる。

【０００６】本発明は、このような課題を解決しようとするものであり、その目的は、ディジタル伝送路を使用し、データ情報を転送する場合にあたって好適な秘話通信の認証と鍵共有の方法を提供するものである。

【０００７】

【課題を解決するための手段】本発明では、各端末装置は、端末装置自身が正しいことを証明するための情報として、端末の識別名と端末の公開鍵暗号方式におけるパブリック鍵とで構成されたディジタル情報に対して証明機関の公開鍵暗号方式のプライベート鍵によりディジタル署名された証明書を保持する。この証明書を保持する端末装置相互が秘話通信を行うとき、各端末装置は、以下のようにして、まず、端末装置が保持する証明書を相互に交換して相手が正しいと認証し、次に、通信データの内容の暗号化／復号に使用するための秘密鍵暗号方式における秘密鍵を公開鍵暗号方式を使用して共有し、この相互に共有した通信用の秘密鍵を使用して秘話通信を行う。

【０００８】端末装置Ｔｉと端末装置Ｔｊが秘話通信を行うとする。まず、端末装置Ｔｉ，Ｔｊは相互に認証を行うための通信路を開設し、自分を証明する証明書Ｃｉ，Ｃｊを互いに交換し検証することで、相手が正しいことを確認するとともに認証のために開設した通信路が正しいことを確認する。

【０００９】次に、認証のために開設した通信路の上位に通信データの内容の暗号化／復号を行うための通信路を開設し、通信データの内容の暗号化／復号のための秘密鍵を共有するために、端末装置Ｔｉは乱数Ｒｋｖｉを発生し、該乱数Ｒｋｖｉを端末装置Ｔｊの認証時に取得した証明書Ｃｊから取り出した端末装置Ｔｊのパブリック鍵を使用して暗号化するとともに、該暗号化データまたは該暗号化データをハッシュしたデータに対して端末装置Ｔｉのプライベート鍵で暗号化することでディジタル署名を行い、これら暗号化データとディジタル署名データのディジタル情報を端末装置Ｔｊに送信する。

【００１０】このディジタル情報を受信した端末装置Ｔｊは、受信したディジタル情報中の端末装置Ｔｊのパブリック鍵により暗号化された乱数Ｒｋｖｉのディジタルデータを端末装置Ｔｊのプライベート鍵により復号することにより乱数Ｒｋｖｉの値を得るとともに、ディジタル署名

データを端末装置Ｔｉの認証時に取得した証明書Ｃｉから取り出した端末装置Ｔｉのパブリック鍵を使用して復号し、該復号したディジタルデータと前記端末装置Ｔｊのパブリック鍵により暗号化された乱数Ｒｋｖｉのディジタルデータを比較し、等しければ正しく端末装置Ｔｉより送信された秘密鍵情報であると確認する。次に、端末装置Ｔｊは乱数Ｒｋｖｊを生成し、この乱数Ｒｋｖｊと復号した乱数Ｒｋｖｉとで排他的論和をとり、該排他的論和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータ（初期値）とする。さらに、端末装置Ｔｊは、該乱数Ｒｋｖｊを端末Ｔｉの認証時に取得した証明書から取り出した端末Ｔｉのパブリック鍵を使用して暗号化するとともに、該暗号化データまたは該暗号化データをハッシュしたデータに対して端末装置Ｔｊのプライベート鍵で暗号化することでディジタル署名を行い、これら暗号化データとディジタル署名データのディジタル情報を端末装置Ｔｉに送信する。

【００１１】このディジタル情報を受信した端末装置Ｔｉは受信したディジタル情報中の端末装置Ｔｉのパブリック鍵により暗号化された乱数Ｒｋｖｊのディジタルデータを端末装置Ｔｉのプライベート鍵により復号することにより乱数Ｒｋｖｊの値を得るとともに、ディジタル署名データを端末装置Ｔｊの認証時に取得した証明書Ｃｊから取り出した端末装置Ｔｊのパブリック鍵を使用して復号し、該復号したディジタルデータと前記端末装置Ｔｊのパブリック鍵により暗号化された乱数Ｒｋｖｊのディジタルデータを比較し、等しければ正しく端末装置Ｔｊより送信された秘密鍵情報であると確認する。次に、端末装置Ｔｉは、先に生成した乱数Ｒｋｖｉと、乱数Ｒｋｖｊとで排他的論理和をとり、該排他的論理和結果を秘密鍵暗号方式で通信するための秘密鍵とその他の必要なデータ（初期値）とする。

【００１２】これにより、端末装置Ｔｉと端末装置Ｔｊは、互いに等しい通信データの内容の暗号化に使用する秘密鍵とその他のデータ（初期値）を共有し、これらの共有した秘密鍵と他のデータを使用して秘密鍵暗号方式で通信内容の暗号化ならびに復号化を行う。

【００１３】また、本発明では、通信データの内容の暗号化／復号の通信路は、認証のために開設した通信路の上位に複数本開設可能し、各通信データの内容の暗号化／復号の通信路で秘話通信を行うときは、各々の通信データの内容の暗号化／復号のための通信路で秘密鍵を共有することで、一つの認証のための通信路上で、各々異なる秘密鍵を使用して複数の通信路で秘話通信が可能とする。

【００１４】さらに、本発明では、通信データの内容の暗号化／復号のための通信路が、認証のための通信路の上位に少なくともひとつ開設してあれば、該認証ための通信路上に新しい通信データの内容の暗号化／復号のための通信路を開設するとき、秘話通信を行うために新たに必要な秘密鍵と他のデータを共有するために使用する証明書の情報は、既に開設している認証路の証明書の情報を使用する。

【００１５】さらに、本発明では、秘話通信を終了するときは、認証のための通信路上に開設された全ての通信データの内容の暗号化／復号のための通信路が閉設されたときに、該認証のための通信路上の情報を閉設する。

【００１６】

【実施例】以下、図面を参照して本発明の一実施例を説明する。なお、本実施例の説明ではディジタル伝送路としてＩＳＤＮを用いるが、勿論、ＩＳＤＮ以外のディジタル伝送路でも適用可能である。

【００１７】図１は、本発明の秘話通信方法が適用される通信システムの一実施例を示すブロック図である。図１において、交換装置１０は複数のＩＳＤＮ基本インタフェース加入者回線を収容している。端末装置２０、３０は該ＩＳＤＮ基本インタフェース加入者回線に接続されている。各端末装置は、ＩＳＤＮ加入者回線のレイヤ１～レイヤ３制御およびレイヤ４から上の上位レイヤのネットワーク制御を行う端末制御部１１０、端末相互の認証処理や鍵共有処理を行う暗号処理部１２０、共有した秘密鍵を使用して秘話通信を行う通信データ処理部１３０から構成されている。端末装置２０、３０は証明機関４０とも接続され、端末の識別名と端末のパブリック鍵で構成されたディジタル情報に対し、当該証明機関４０のプライベート鍵によりディジタル署名された証明書の発行を受ける。なお、利用者が直接、証明機関４０におもむいて証明書の発行を受ける場合には、端末装置２０、３０と証明機関４０間の接続を省略できる。以下では、端末装置２０をＴｉ、端末装置３０をＴｊとする。

【００１８】図２に、本実施例の説明で使用する記号の一例を示す。なお、端末Ｔｊに関しては、図２の記号中の「ｉ」を「ｊ」に置き替えればよい。

【００１９】図３は、証明機関４０が作成する証明書の一例である。これは端末Ｔｉの証明書Ｃｉの例を示したもので、証明書の長さＣＤＬと、端末装置の識別名Ｔｉと、端末Ｔｉの公開鍵暗号方式におけるパブリック鍵Ｐｋｉと、該ＴｉとＰｋｉを結合した情報に対して一方向性のデータ圧縮関数Ｈでハッシュし、その値を当該証明機関４０の公開鍵暗号方式のプライベート鍵Ｓｃａで暗号化した暗号文Ｅ[Ｓｃａ](Ｈ(Ｔｉ‖Ｐｋｉ))、すなわち、ディジタル署名されたデータで構成される。ここで、公開鍵暗号方式としては、代表的なものにＲＳＡ暗号方式（詳細は、文献［６］：「ＰＫＣＳ＃１ ＲＳＡ Encryption Standard, Version1. ５, ＲＳＡ DataSecurity Inc. １９９３」を参照）があり、秘密鍵暗号方式としては、ＤＥＳ方式（詳細は、文献［７］：「ＦＩＰＳ Publication ４６－１：DataEncryption Standard, National Bureau of Standards. １９８８」を参照）がある。また、ハッシュ関数としては、ＭＤ２（詳細

は、文献［８］：「ＲＦＣ１３１９：The MD2 Message-Digest Algorithm., B. Kaliski., １９９２」を参照）やＭＤＳ５（詳細は、文献［９］：「ＲＦＣ１３２１：TheMD５Message-Digest Algorithm., B. Kaliski., １９９２」を参照）などがある。なお、本発明は、他の公開鍵暗号方式、秘密鍵暗号方式、ハッシュ関数に適用可能なことはもちろんである。

【００２０】端末設置時に、端末装置２０（端末Ｔi）は、当該端末のパブリック鍵Ｐkiとプライベート鍵Ｓkiを生成するとともに、該端末の識別名ＴiとパブリックＰkiを証明機関４０に送って証明書Ｃiの発行の受け、該端末のプライベート鍵Ｓki、図２に示す証明書Ｃi、証明機関４０のパブリック鍵Ｐcaを暗号処理部１２０に設定する。同様に、端末装置３０（端末Ｔj）でも、該端末のプライベート鍵Ｓkj、証明書Ｃj、証明機関４０のパブリック鍵Ｐcaを暗号処理部１２０に設定する。

【００２１】端末装置２０（Ｔi）と端末装置３０（Ｔj）が秘話通信を行うとき、まず、各端末が保持する証明書Ｃi、Ｃjを相互に交換して相手が正しいことを認証し、次に、通信データの内容の暗号化／復号に使用するための秘話鍵暗号方式における秘密鍵を公開鍵暗号方式を使用して共有し、この相互に共有した秘話鍵を使用して秘話通信を行う。

【００２２】初めに、図４を用いて端末相互の認証手順を説明する。この段階ではすでに、端末Ｔiは当該端末のプライベート鍵Ｓki、証明書Ｃi、証明機関のパブリック鍵Ｐcaを保持し、端末Ｔjでも当該端末のＳkj、Ｃjおよび証明機関のＰcaを保持している。

【００２３】①　端末Ｔiは乱数Ｒiを生成し、端末ＴjにＣi‖Ｒiを送信する。

②　端末Ｔjは、受信した証明書Ｃiを以下の通りに検査し、正しいことを確かめる。

ａ．受信したＣi中のＴi，ＰkjからＨ(Ｔi‖Ｐki)を計算する。

ｂ．受信したＣi中のディジタル署名データからＥ[Ｐca](Ｅ[Ｓca]Ｈ(Ｔi‖Ｐki))を計算し、Ｈ(Ｔi‖Ｐki)を得る。

ｃ．上記ａとｂの計算値が等しいか検査し、等しいなら、受信した証明書Ｃiは正しいと確認する。そして、正しいと確認されたなら、受信した証明書Ｃiを保持する。

【００２４】③　端末Ｔjは乱数Ｒjを生成し、端末ＴiにＣj‖Ｒjを送信する。

④　端末Ｔiは、受信した証明書Ｃjを以下の通りに検査して、正しいことを確かめる。

ａ．受信したＣj中のＴj，ＰkjからＨ(Ｔj‖Ｐkj)を計算する。

ｂ．受信したＣj中のディジタル署名データからＥ[Ｐca](Ｅ[Ｓca]Ｈ(Ｔj‖Ｐkj))を計算し、Ｈ(Ｔj‖Ｐkj)を得る。

ｃ．上記ａとｂの計算値が等しいか検査し、等しいなら、受信した証明書Ｃjは正しいと確認する。そして、正しいと確認されたらな、受信した証明書Ｃjを保持する。

【００２５】⑤　端末Ｔjは端末Ｔiに、Ｒj，Ｒi，Ｔiの平文データとその暗号化データを結合したＲj‖Ｒi‖Ｔi‖Ｅ[Ｓkj](Ｒj‖Ｒi‖Ｔi)を送信する。

⑥　端末Ｔiは、受信した情報を以下の通りに検査し、端末Ｔjが正しいことを確かめる。

ａ．受信した暗号化データからＥ[Ｐkj](Ｅ[Ｓkj](Ｒj‖Ｒi‖Ｔi)を計算し、Ｒj‖Ｒi‖Ｔiを得る。

ｂ．受信した平文データのＲj‖Ｒi‖Ｔiと、上記ａで得たＲj‖Ｒi‖Ｔiとを比較する。等しければ、端末Ｔjが正しいと確認する。

【００２６】⑦　端末Ｔiは端末Ｔjに、Ｒi，Ｒj，Ｔjの平文データとその暗号化データを結合したＲi‖Ｒj‖Ｔj‖Ｅ[Ｓki](Ｒi‖Ｒj‖Ｔj)を送信する。

⑧　端末Ｔjは、受信した情報を以下の通りに検査し、端末Ｔiが正しいことを確かめる。

ａ．受信した暗号化データからＥ[Ｐki](Ｅ[Ｓki](Ｒi‖Ｒj‖Ｔj)を計算し、Ｒi‖Ｒj‖Ｔjを得る。

ｂ．受信した平文データ中のＲi‖Ｒj‖Ｔjと、上記ａで得たＲi‖Ｒj‖Ｔjとを比較する。等しければ、端末Ｔiが正しいと確認する。

【００２７】次に、図５を用いて、通信データの内容の暗号化／復号のために使用する秘密鍵とその他の必要データ（初期値）の共有手順について説明する。この段階では、端末Ｔiは当該端末の証明書ＣiにＣiに加えて相手端末Ｔjの証明書Ｃjを保持し、同様に端末Ｔjでも当該端末のＣjに加えて相手端末ＴiのＣjを保持している。

【００２８】①　端末Ｔiは乱数Ｒkviを生成し、端末ＴjにＲkviの暗号化データとそのディジタル署名データを結合したＥ[Ｐkj](Ｒkvi)‖Ｅ[Ｓki](Ｈ(Ｅ[Ｐkj](Ｒkvi)))を送信する。

②　端末Ｔjは、受信した情報を以下の通りに検査して、情報が正しいことを確かめ、データ暗号化鍵と初期値を生成する。

ａ．受信したディジタル署名データからＥ[Ｐki](Ｅ[Ｓki](Ｈ(Ｅ[Ｐkj](Ｒkvi))))を計算し、Ｈ(Ｅ[Ｐkj](Ｒkvi)))を得る。

ｂ．受信した暗号化データからＨ(Ｅ[Ｐkj](Ｒkvi))を計算し、上記ａで得たＨ(Ｅ[Ｐkj](Ｒkvi))と比較し、等しければ、メッセージが改ざんされていないと確認する。

ｃ．Ｅ[Ｓkj](Ｅ[Ｐkj](Ｒkvi))を計算し、Ｒkviを得る。

ｄ．乱数Ｒkvjを生成する。そして、上記ｃで復号した乱数Ｒkviと生成した乱数Ｒkvjとで排他的論理和を取り、以下の通りにデータ暗号化／復号鍵ＤＥＫs、初期

値ＩＶｓを生成する。
ＤＥＫｓ：RkviとRkvjの排他的論理和データの上位８バイト
ＩＶｓ　：RkviとRkvjの排他的論理和データの下位８バイト
ｅ．ＤＥＫｓとＩＶｓを通信データ処理部１３０へ設定する。
【００２９】③　端末Ｔjは端末Ｔiに、Rkvjの暗号化データとそのディジタル署名データを結合したＥ[Pki](Rkvj)‖Ｅ[Skj](Ｈ(Ｅ[Pki](Rkvj)))を送信する。
④　端末Ｔiは、受信した情報を以下の通りに検査して、情報が正しいことを確かめ、データ暗号化鍵と初期値を生成する。
ａ．受信したディジタル署名データからＥ[Pkj](Ｅ[Skj](Ｈ(Ｅ[Pki](Rkvj))))を計算し、Ｈ(Ｅ[Pki](Rkvj))を得る。
ｂ．受信した暗号化データからＨ(Ｅ[Pki](Rkvj))を計算し、上記ａで復号したＨ(Ｅ[Pki](Rkvj))と比較し、等しければ、メッセージが改ざんされていないと確認する。
ｃ．Ｅ[Ski](Ｅ[Pki](Rkvj))を計算し、Rkvjを得る。
ｄ．上記ｃで復号した乱数Rkvjと先に生成した乱数Rkviとで排他的論理和を取り、以下の通りにデータ暗号化／復号鍵ＤＥＫｓ、初期値ＩＶｓを生成する。
ＤＥＫｓ：RkviとRkvjの排他的論理和データの上位８バイト
ＩＶｓ　：RkviとRkvjの排他的論理和データの下位８バイト
ｅ．ＤＥＫｓとＩＶｓを通信データ処理部１３０へ設定する。
【００３０】以後、端末Ｔiと端末Ｔjは、共有した暗号化／復号のための秘密鍵ＤＥＫｓとその初期値ＩＶｓを使用して通信データの暗号化／復号を行う。例えば、端末Ｔiが送信側、端末Ｔjが受信側の場合、端末Ｔiは平文（通信データ）ｐを鍵ＤＥＫｓ、初期値ＩＶｓで秘密鍵暗号方式により暗号化した暗号文ｅ[ＤＥＫｓ，ＩＶｓ](ｐ)を生成して送信し、端末Ｔjは、受信した暗号文について同じくＤＥＫｓ，ＩＶｓで秘密鍵暗号方式によりｄ[ＤＥＫｓ，ＩＶｓ](ｅ(ＤＥＫｓ，ＩＶｓ](ｐ))を計算して、平文ｐを復号する。
【００３１】次に、図４の認証のための通信路ならびに図５の通信路が既に確立し、端末Ｔiと端末Ｔjの間で通信データの内容の暗号化／復号を行っているときに、同じ端末間で新たな秘話通信要求が発生した場合の動作について、図６により説明する。端末ＴiならびにＴjは、互いに認証した相手端末の証明書ＣjあるいはＣi（以下では、Ｃを総称する）に加えて、認証のための通信路がどの端末と確立されているかを示すカウンタフラグＦlgjあるいはＦigi（以下では、Ｆlgで総称する）を保持している。初期状態ではカウンタフラグＦlg、証明書Ｃともゼロである。図６では、ＦlgとＣが各々１個しか示されていないが、もちろん複数の端末と同時に秘話通信を行うために、複数のカウンタフラグＦlgと証明書Ｃを保有することが可能である。
【００３２】秘話通信の要求が発生したとき、端末はカウンタフラグＦlgがゼロ以上かどうかと、ゼロ以上ならどの端末であるかを示す情報を含む証明書Ｃを検査することにより、端末の動作を決定する。すなわち、新たに秘話通信の要求が発生としたとき、Ｆlgを検査し、ゼロ以上かどうか調べる。Ｆlgがひとつもゼロ以上でないなら、または、Ｆlgがゼロ以上でも、保有している証明書Ｃを検査した結果、秘話通信を行う相手の証明書Ｃを保持していないなら、新しい端末との秘話通信要求とし、前記の図４と図５の手順を実行して端末相互の認証と通信データの内容の暗号化／復号を行うための鍵を共有し、秘話通信を行う。図６（ａ）はこれを示したもので、便宜上、ここでは端末相互の認証手順のみを示している。このとき、Ｆlgの内容は１加算するとともに、獲得した対応する端末の証明書Ｃを保持機構に設定する。
【００３３】一方、新たに秘話通信の要求が発生したとき、検査したＦlgがゼロ以上でかつ、秘話通信を行う相手の証明書Ｃを既に保持しているなら、対応するＦlgの内容を１加算するとともに、図３で確立した認証のための通信路上で、直ちに図５の鍵共有手順を実行し、新たな通信データの暗号化／復号のための通信路を確立するとともに、この通信路上で秘話通信を行うための鍵を共有する。このとき、相手端末の証明書Ｃは、既に保持している証明書を使用し、端末相互の新たな証明書はの交換は実行しない。図６（ｂ）はこれを示している。
【００３４】このようにすることにより、端末相互で１本の物理チャネル上に複数の論理パスを開設して秘話通信を行う場合においても、端末相互の認証は最初の１回で終了するとともに、論理パスごとに異なる鍵で通信データの暗号化／復号を実行することができる。
【００３５】次に、秘話通信を終了する場合について説明する。秘話通信を終了するときは、その要求にもとづき、まず最初に該通信データの内容の暗号化／復号のための通信路を閉設する。次に、図６に示したカウンタフラグＦlgにおいて、閉設した相手端末に対応するＦlgの内容を１減算する。減算した結果がゼロ以上なら、図４で確立した認証のための通信路はそのままとし、その秘話通信終了のための要求動作を終了する。もしＦlgの内容を１減算した結果がゼロなら、獲得している対応する端末の証明書Ｃの内容を初期化（クリア）するとともに、相手端末に対応する開設している図４の認証のための通信路を閉設することで、その秘話通信終了のための要求動作を終了する。
【００３６】このようにすることにより、図４の認証の

ための通信路の上に複数の通信データの内容の暗号化／復号のための通信路が開設されているときは、認証のための通信路をそのままにできるので、上記の、図４の認証のための通信路ならびに図５の通信路が既に確立し、通信データの内容の暗号化／復号を行っているときに、同じ端末間で新たな秘話通信要求が発生した場合の動作が実行できる。

【００３７】

【発明の効果】以上のように、本発明の認証および鍵共有方法によれば、既に秘話通信を行っている端末相互で、新たな論理パスを生成して秘話通信を行う特には、再度端末相互の認証を行う必要がないためオーバヘッドがなく、また、証明書の通信データの内容の暗号化／復号のための通信路パス相互で矛盾を生じないという利点がある。

【図面の簡単な説明】

【図１】本発明の秘話通信方法が適用される通信システムの一実施例を示すブロック図である。

【図２】本発明の実施例に使用する記号とその意味の一例を示す図である。

【図３】本発明で使用する証明書の一を示す図である。

【図４】本発明による端末相互の認証手順を説明するための図である。

【図５】本発明による秘密鍵共有手順を説明するための図である。

【図６】本発明による新たな秘話通信要求が発生した場合の認証／秘密鍵共有手順を説明するための図である。

【符号の説明】

１０　交換装置

２０，３０　端末装置

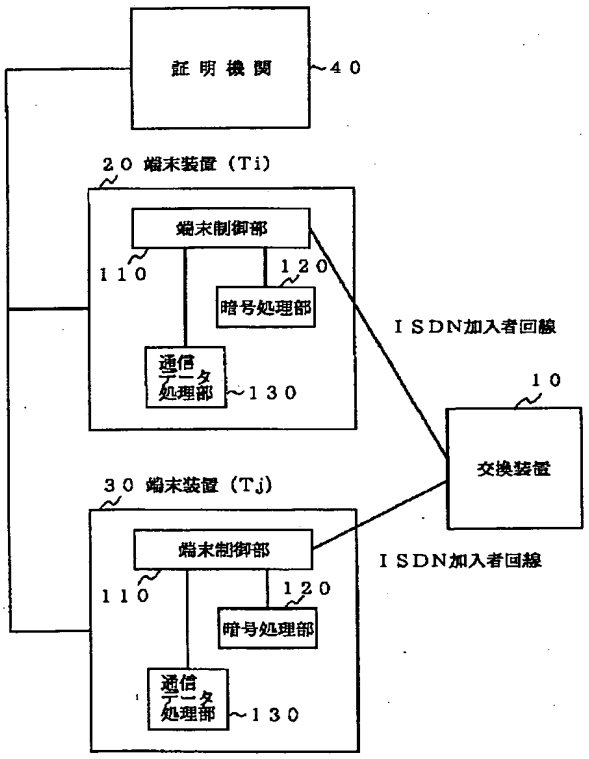
４０　証明機関

１１０　端末制御部

１２０　暗号化処理部

１３０　通信データ処理部

【図１】



【図２】

記　　号	意　　味
Ti	端末Tiの識別名
Ri，Rkvi	端末Tiが発生する乱数
Ski	端末Tiのプライベート鍵
Pki	端末Tiのパブリック鍵
Sca	証明機関のプライベート鍵
Pca	証明機関のパブリック鍵
DEKs	通信データの内容の暗号化／復号鍵に使用する秘密鍵
IVs	通信データの内容の暗号化／復号のための初期値
e[DEKs, IVs](p)	平文ｐを鍵DEKs、初期値IVsで秘密鍵暗号方式により暗号化した暗号文
d[DEKs, IVs](c)	暗号文ｃを鍵DEKs、初期値IVsで秘密鍵暗号方式により復号した平文
E[Ski](p)	文ｐを鍵Skiで公開鍵暗号方式により暗号処理した暗号文
E[Pki](E[Ski](p)	暗号文E[Ski](p) を鍵Pkiで公開鍵暗号方式により復号処理した復号文
H(p)	文ｐを関数Hでハッシュした値
‖	結合
Ci	端末Tiの証明書

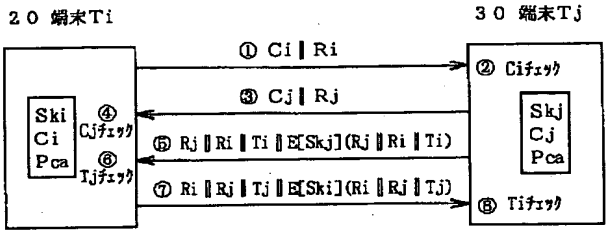
【図３】

端末Tiの証明書Ci

CDL
Ti
Pki
E[Sca] (H(Ti‖Pki))

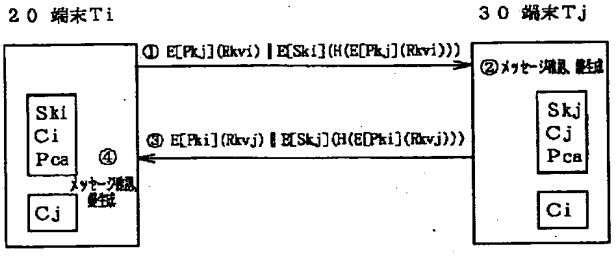
【図４】

端末相互の認証手順



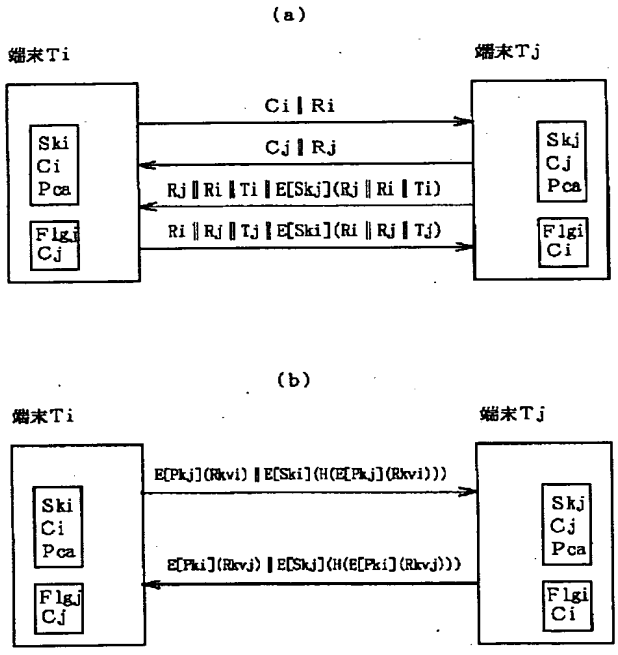
【図５】

鍵 共 有 手 順



【図６】

端末相互の認証／鍵共有手順



フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/32			H04L 9/00	601E
				673B
				675A

(72)発明者　青木　克彦
東京都武蔵野市吉祥寺本町１丁目14番５号
エヌティティエレクトロニクステクノロジー株式会社内